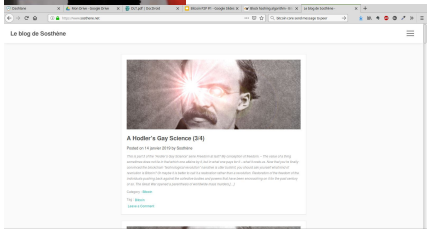
Bitcoin P2P

bisq, l’exchange décentralisé

Pourquoi bisq ?

1. Le seul exchange *vraiment* décentralisé
2. Quels sont les compromis par rapport à un exchange normal ?
3. Un nouveau modèle de gouvernance ?

www.sosthene.net
@Sosthene@bitcoinhackers.org



Comment obtenir des bitcoins ?

- les miner
- les voler
- les gagner
- les acheter :
  - en cash, face à face
  - à distance à des inconnus
  - à un service centralisé (= “exchange”)

Pourquoi des exchanges centralisés ?

- Responsabilité : la plupart des utilisateurs ne sont pas prêt à assumer les risques qu'implique la transaction de bitcoins en P2P
- Liquidité : le modèle centralisé permet de concentrer les acheteurs et les vendeurs et de créer un marché plus liquide
- Simplicité d'utilisation : l'utilisation de Bitcoin nécessite une culture qui est encore peu répandue dans la société aujourd'hui (cryptographie asymétrique, conservation de clés, bonnes pratiques de sécurité sur internet…)
- Business : il y a beaucoup d'argent à se faire en se plaçant dans le rôle d'intermédiaire des transactions. La décentralisation n'a pas beaucoup de sens d'un point de vue business

Trusted Third Parties are Security Holes

Nick Szabo

Originally published in 2001

Introduction

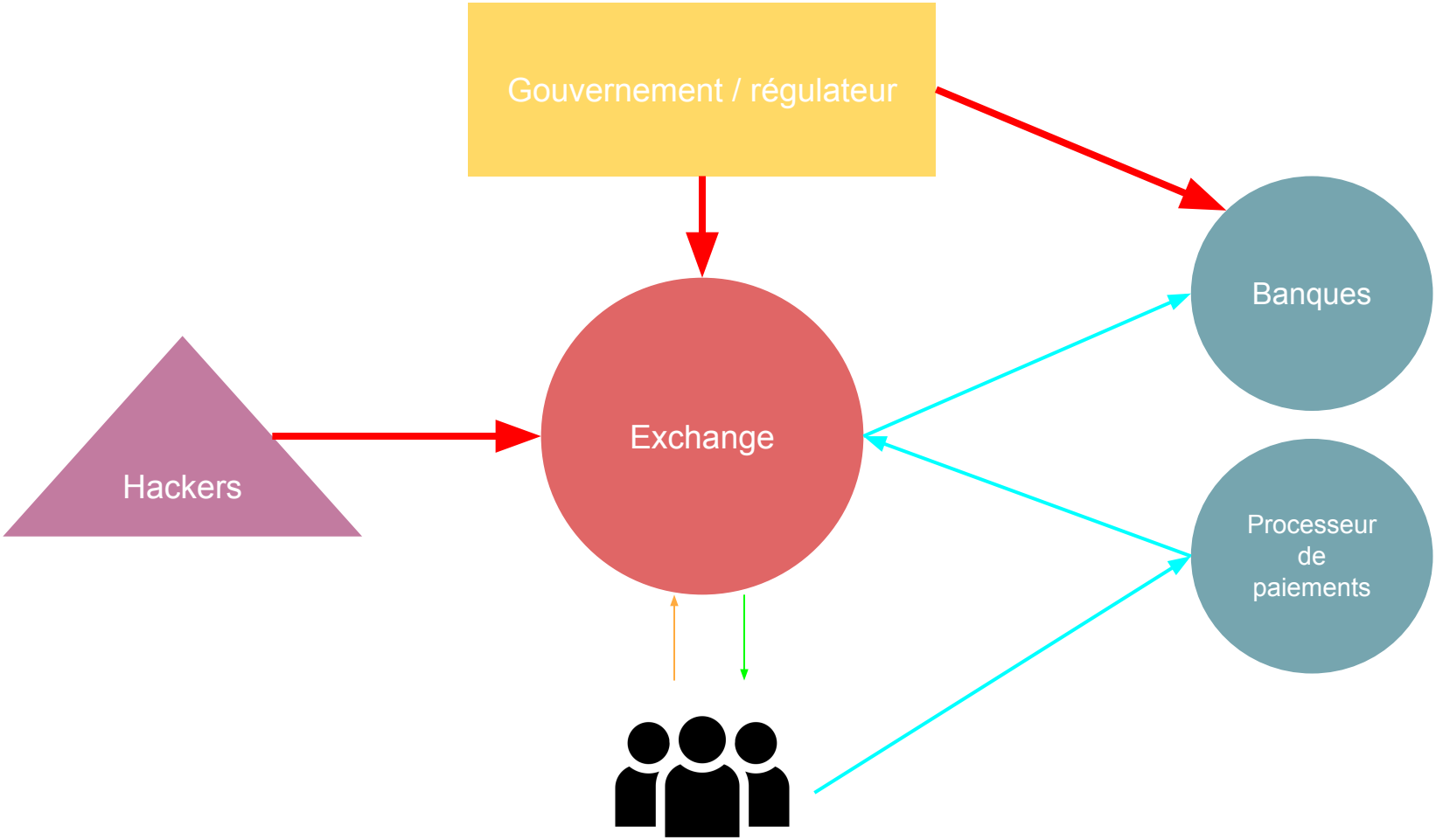
Commercial security is a matter of solving the practical problems of business relationships such as privacy, integrity, protecting property, or detecting breach of contract. A security hole is any weakness that increases the risk of violating these goals. In this real world view of security, a problem does not dissapear because a designer assumes it away. The invocation or assumption in a security protocol design of a "trusted third party" (TTP) or a "trusted computing base" (TCB) controlled by a third party constitutes the introduction of a security hole into that design. The security hole will then need to be plugged by other means.

If the risks and costs of TTP institutional alternatives were not accounted for in the protocol design, the resulting protocol will in most cases be too costly or risky to be practical. If the protocol beats these odds and

Le problème avec les exchanges centralisés

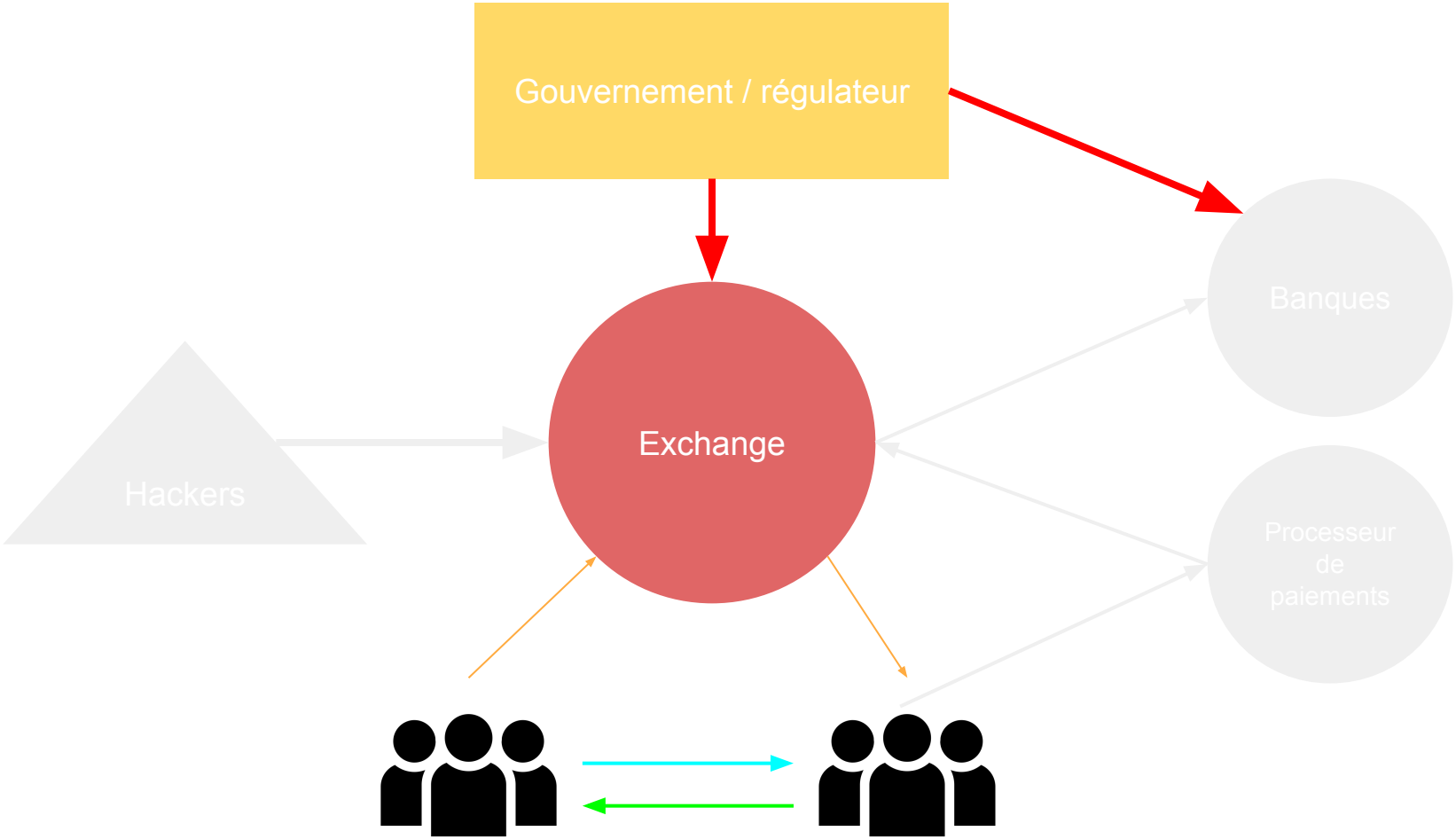
- Peu de différences avec le système bancaire traditionnel :
  - Transparence de toutes les transactions
  - Rigidité des contraintes réglementaires (KYC/LAB/FT…)
  - Censure de transaction, gel des avoirs, dénonciation au fisc...
  - Pratique plus ou moins assumé de la réserve fractionnaire, avec tous les risques de faillites que cela implique
  - “honey pot” massif pour tous les hackers du monde
  - Hostilité du système bancaire et financier traditionnel (cf gel des comptes de Gatecoin à HK)
  - Déjà une dette technique (Coinbase incapable de batcher ses transactions en 2017)
  - Les problèmes des plateformes deviennent des défauts de Bitcoin dans l’esprit du grand public
- Peu de recours en cas de fraude ou d’arnaque (MtGox, Quadriga…)
- Perpétuent les mauvaises pratiques du système financier traditionnel

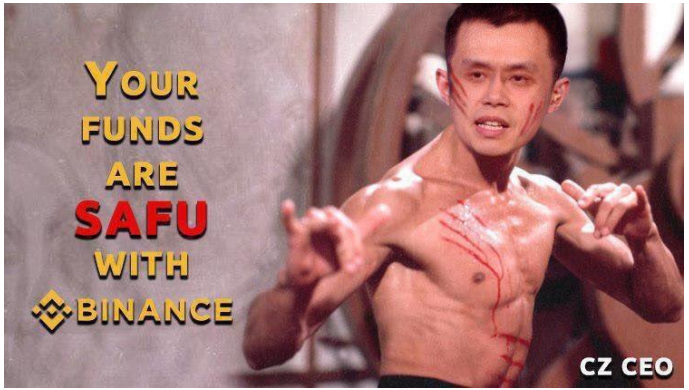
➔ **Sous leur forme actuelle, les exchanges sont d’énormes SPOF, l’ écosystème Bitcoin construit autour d’eux ne vaut guère mieux que le système bancaire traditionnel**


Gouvernement / régulateur
Banques
Hackers
Exchange
Processeur
de
paiements

L’exchange P2P : LocalBitcoin

- Plateforme finlandaise créée en 2012 et qui se distinguait encore il y a peu en n’étant relativement peu intrusive (pas de KYC)
- Services :
  - Mise en relation d’acheteurs et de vendeurs (système d’offres)
  - Séquestre
  - Réputation
- Possibilité d’échange en cash irl
- Prix souvent moins attractifs


Gouvernement / régulateur
Banques
Exchange
Hackers
Processeur de paiements



Any use as described in this paragraph shall constitute a "Prohibited Use". If Binance determines that you have engaged in any Prohibited Use via the Site, Binance may address such Prohibited Use through an appropriate sanction, in its sole and absolute discretion. Such sanction may include, but is not limited to, making a report to law enforcement or other authorities; proposal to Binance Chain governance (Validators and Community) for confiscation of any Digital Tokens obtained in any Prohibited Use; and, terminating your access to any Services through the Site. In addition, Binance makes no representation or warranty as to what actions Binance Chain governance (Validators and Community) may take, at its sole and absolute discretion, including to seize and hand over your property to law enforcement or other authorities where circumstances warrant.

7. Anti-Money Laundering and Counter-Terrorist Financing: Binance is committed to providing you with safe, compliant, and reputable Services. Accordingly, Binance insists on a comprehensive and thorough user due diligence process and implementation and ongoing analysis and reporting. This includes monitoring of and for suspicious transactions and mandatory reporting to international regulators. Binance needs to keep certain information and documentation on file pursuant to applicable law and its contractual relationships, and Binance hereby expressly reserves the right to keep such information and documentation. This will apply even when you terminate your relationship with Binance or abandon your wallet and related applications.

Binance and Binance Chain community reserves the right to refuse service of the Site, or to bar transactions from or to, or terminate any relationship with, any user for any reason (or for no reason) at any time. Without limiting the generality of the foregoing, this includes, but is not limited to, anyone from or in jurisdictions that do not meet international AML/CTF standards as set out by the FATF; anyone that is a Politically Exposed Person within the meaning of the FATF's 40 Recommendations; or, anyone that fails to meet any user due diligence standards, requests, or requirements of Binance and Binance Chain community. At all times, you may be subject to enhanced user due diligence procedures in your use of the Site and any Service.
7. Your Representations & Warranties: You represent and warrant to Binance and Binance Chain community as follows:

7.1. that, if you are an individual user, you are 18 years of age or older and that you have the capacity to contract under applicable law;
7.2. that, if you are not an individual user, you have the requisite power and authority to sign and enter into binding agreements for and on behalf of the user;
7.3. that you understand the risks associated with using the Site, that you are not barred from using the Site by paragraph 3 of these Terms, and that you are not otherwise

bisq

- bisq n’est pas une personne morale, il n’y a pas d’entreprise derrière le software
- Avantage :
  - Plus de point de pression pour le régulateur
  - Pas de possibilité de censure ou de gel de transactions
- Inconvénient :
  - Incitations : comment inciter les développeurs à travailler sur le projet ?
  - Tous les échanges impliquent transaction fiat et/ou crypto (on perd le côté instantané des exchanges centralisés)
  - UI et support : en cas de problème, il existe aujourd’hui des arbitres, mais ils sont voués à disparaître prochainement. En cas de conflit, les utilisateurs devront essayer de s’accorder et désigner un médiateur si ce n’est pas possible

Acheter des bitcoins - le process

1. Sélectionner une offre
2. Envoyer une certaine somme en bitcoins comprenant :
   a. un dépôt de sécurité (une sorte de caution)
   b. les frais de trade (aujourd'hui ils vont à l'arbitre)
   c. les frais de minage
3. Une fois la transaction confirmée, faire le paiement (SEPA, Revolut, autre…)
4. Le vendeur confirme le paiement, vous recevez vos bitcoins avec votre dépôt de sécurité

La DAO

- Pour répondre au problème des incitations les fondateurs de bisq ont décidé de créer une DAO avec un token
- Le principe est le suivant :
  - un développeur travaille sur le code de bisq
  - Il fait une demande de bsq (le token) dans la DAO, et fournit une quantité équivalente de satoshis (le bsq est en fait un colored coin)
  - Si la demande est acceptée, le développeur possède désormais des bsq
  - Des traders achètent les bsq contre de l'argent (fiat ou btc)
  - les frais de service sont moins élevés en bsq qu'en btc, créant ainsi une incitation à les utiliser
  - les bsq consommés sont détruits ("dé-colorié")
  - L'accès à certaine fonction nécessite de déposer une caution en bsq
  - La possession de bsq détermine également le poids du vote de chacun